(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2002－513245
（P2002－513245A）
(43)公表日　平成14年５月８日(2002.5.8)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/46		Ｈ０４Ｌ　11/00	３１０Ｃ	
12/28		11/18		
12/18				

審査請求　未請求　予備審査請求　有　（全 55 頁）

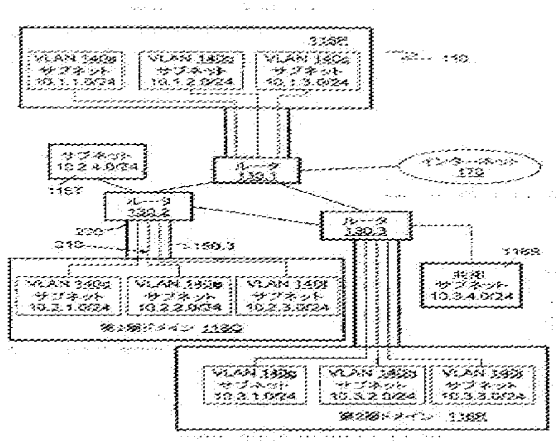
(21)出願番号　特願2000－546493(P2000－546493)
(86)（22)出願日　平成11年４月22日(1999.4.22)
(85)翻訳文提出日　平成12年10月12日(2000.10.12)
(86)国際出願番号　ＰＣＴ／ＵＳ９９／０８８６６
(87)国際公開番号　ＷＯ９９／５６４３６
(87)国際公開日　平成11年11月４日(1999.11.4)
(31)優先権主張番号　０９／０６７，７６１
(32)優先日　平成10年４月27日(1998.4.27)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　インターエヌエイピー・ネットワーク・サービシーズ・コーポレイション
ＩｎｔｅｒＮＡＰ　Ｎｅｔｗｏｒｋ　Ｓｅｒｖｉｃｅｓ　Ｃｏｒｐｏｒａｔｉｏｎ
アメリカ合衆国ワシントン州98101－4064・シアトル・スイート　1000・テンスフロア・ツーユニオンスクエア・ユニオンストリート　601
(72)発明者　マクニール、トーマス・ジー
アメリカ合衆国ユタ州84097・オーレム・イースト　1000ノース　1072
(74)代理人　弁理士　大島　陽一

最終頁に続く

(54)【発明の名称】　ネットワークにおける接続の確立

(57)【要約】
幾つかのドメイン（「第2層ドメイン」）を含む所定のネットワークが、ルータによって相互接続される。各ドメインにおいて、トラフィックはMACアドレス（又は、他のデータリンク層アドレス）に基づき送信される。ルータは、IPアドレス又は他のネットワーク層アドレスに基づきトラフィックの経路を指定する。ネットワークの接続を制限するために、ネットワーク管理者は、通信を許可されたサブネットワークの集まりである各接続グループを指定する。また、管理者は、どのエンティティ（MACアドレス、ポート、又はユーザ名）が同じグループに属するかを指定する。そのエンティティは、同一のドメインか或いは異なるドメインに存在し得る。コンピュータシステムは、ルータに対してアクセス制御リストを自動的に作成し、管理者の指定に従ってトラフィックを許容又は拒否する。また、コンピュータシステムはVLANを生成し、指定に従ってトラフィックを許可又は拒否する。ここで、各VLANはドメインの一部か或いはドメイン全体である。各ドメインにおける接続性はVLANにより制限され、またドメイン間の接続性はアクセス制御リスト



【特許請求の範囲】

【請求項１】　ネットワーク端末をバーチャル同報通信ドメイン（VBDs）に接続するための方法であって、

ネットワーク上においてネットワーク端末のユーザを識別する情報を前記ネットワーク端末から受信する過程と、

1以上のVBDを含むユーザの属する接続グループを決定する過程と、

前記ネットワーク端末が接続される1以上のVBDを決定する過程であって、前記1以上のVBDが前記接続グループのメンバであるような前記決定過程と、

前記ネットワーク端末を前記1以上のVBDに接続するためのコマンドを発行する過程とを含むことを特徴とする方法。

【請求項２】　各VBDが、前記トラフィックが生じる前記VBDへの同報通信トラフィックを制限可能なドメインのサブドメインであり、

前記接続グループが、少なくとも2つのドメインからのVBDを含み、

前記ネットワーク端末が接続された1以上のVBDが、前記ネットワーク端末を含む前記ドメインに基づき決定されることを特徴とする請求項１に記載の方法。

【請求項３】　各VBDがVLANであり、また前記ネットワーク端末が、前記接続グループに属するVLAN並びに前記ネットワーク端末を含む前記ドメインに接続されることを特徴とする請求項２に記載の方法。

【請求項４】　ネットワーク端末をバーチャル同報通信ドメイン（VBDs）に接続するための構造体であって、

ネットワーク上においてネットワーク端末のユーザを識別する情報を前記ネットワーク端末から受信する手段と、

1以上のVBDを含むユーザの属する接続グループを決定する手段と、

前記ネットワーク端末が接続される1以上のVBDを決定する手段であって、前記1以上のVBDが前記接続グループのメンバであるような前記決定手段と、

前記ネットワーク端末を前記1以上のVBDに接続するためのコマンドを発行する手段とを含むことを特徴とする構造体。

【請求項５】　各VBDが、前記トラフィックが生じる前記VBDへの同報通信トラフィックを制限可能なドメインのサブドメインであり、

前記接続グループが、少なくとも2つのドメインからのVBDを含み、

前記ネットワーク端末が接続された1以上のVBDが、前記ネットワーク端末を含む前記ドメインに基づき決定されることを特徴とする請求項４に記載の構造体。

【請求項６】　　各VBDがVLANであり、また前記ネットワーク端末が、前記接続グループに属するVLAN並びに前記ネットワーク端末を含む前記ドメインに接続されることを特徴とする請求項５に記載の構造体。

【請求項７】　　前記構造体が、（１）所定のコンピュータシステム、及び（２）前記コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステム及び前記プログラムが、前記決定手段の各々を含むことを特徴とする請求項４に記載の構造体。

【請求項８】　　前記構造体が、所定のコンピュータの読取り可能な媒体であり、そこで各手段が、1以上のコンピュータの命令、コンピュータの読取り可能なデータ、又は1以上の命令及びデータの組合せを含むことを特徴とする請求項４に記載の構造体。

【請求項９】　　ネットワークドメイン間のトラフィックの経路を指定する1以上の装置に対して1以上のアクセス制御リスト（ACLs）を生成するための方法において、そのような装置にACLが与えられた場合に、前記装置が、前記ACLを用いて前記ドメイン間においてどのようなトラフィックが許可及び／又は拒否されるかを決定し、更に、

サブネットワークの各グループ内においてトラフィックが許可されるように、サブネットワークの1以上のグループを規定する過程であって、各サブネットワークがネットワークドメインの一部であるか、或いはネットワークドメインの全てであり、また各グループに対して、所定のコンピュータシステムに前記グループに属するサブネットワークの識別子を与えるような前記過程と、

前記コンピュータシステムが、各グループ内のトラフィックを許可するために1以上のACLを生成する過程とを含むことを特徴とする方法。

【請求項１０】　　前記1以上のACLが異なるグループにおけるサブネットワーク間のトラフィックを拒否する前記複数のグループを規定する過程を含むことを特徴とする請求項９に記載の方法。

【請求項１１】　1以上の共用サブネットワークの識別子を受信する前記コンピュータシステムを更に含む前記方法において、トラフィックが、前記グループの何れか1つにおける各共用ネットワークと任意の別のサブネットワークの間において許可され、

1以上のACLによって、トラフィックが、前記グループの何れか1つにおける前記共用サブネットワークの何れか1つと任意のサブネットワークとの間において許可されることを特徴とする請求項９に記載の方法。

【請求項１２】　少なくとも1つの前記ドメインが、前記ドメインにおけるトラフィックを制限することが可能であるような前記方法であって、

1以上のグループの各々に対して、前記コンピュータシステムが、前記グループ内において許可及び／又は拒否されたトラフィックを識別するための情報を受信する過程であって、前記情報が、制限するトラフィックにおける1以上のドメインによって使用されるような前記受信過程と、

前記情報による指定に従ってトラフィックを許可及び／又は拒否するように、前記コンピュータシステムがトラフィックを制限可能な各ドメインを構成する過程とを更に含むことを特徴とする請求項９に記載の方法。

【請求項１３】　所定のグループ内において許可及び／又は拒否されたトラフィックを識別するための情報が、1以上の（１）トラフィックを制限可能なドメイン内のトラフィックを各々送信する1以上のスイッチのポートであって、前記グループ内のトラフィックを運ぶための前記ポートと、（２）前記グループに属するエンティティの物理的アドレスと、更に（３）前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項１２に記載の方法。

【請求項１４】　各サブネットワークの識別子が、アドレス又はアドレスレンジであることを特徴とする請求項９に記載の方法。

【請求項１５】　前記1以上の装置が、IPアドレスに基づきトラフィックの経路を指定し、また各ドメイン内において、トラフィックが物理的アドレスに基づき端末間で送信されることを特徴とする請求項９に記載の方法。

【請求項１６】　ネットワークドメイン間のトラフィックの経路を指定す

る1以上の装置に対して1以上のアクセス制御リスト（ACLs）を生成するための所定の構造体において、そのような装置にACLが与えられた場合に、前記装置が、前記ACLを用いて前記ドメイン間においてどのようなトラフィックが許可及び／又は拒否されるかを決定し、更に、

各グループ内においてトラフィックが許可されるように、サブネットワークの1以上のグループをコンピュータシステムに対して規定する手段であって、各サブネットワークがネットワークドメインの一部であるか、或いはネットワークドメインの全てであり、また各グループに対して、前記グループに属するサブネットワークの識別子をコンピュータシステムによって読取るための前記規定手段と、

前記コンピュータシステムによって、各グループ内のトラフィックを許可するために1以上のACLを生成するための手段とを含むことを特徴とする構造体。

【請求項１７】　前記構造体が、前記コンピュータシステム及び該コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステムと前記プログラムとの組合せが、前記規定手段及び生成手段を含むことを特徴とする請求項１６に記載の構造体。

【請求項１８】　前記構造体が、前記規定手段及び前記生成手段を実施するための命令を含むコンピュータの読取り可能媒体であることを特徴とする請求項１６に記載の構造体。

【請求項１９】　前記規定手段が複数のグループを規定するときに、前記1以上のACLが異なるグループにおけるサブネットワーク間のトラフィックを拒否することを特徴とする請求項１６に記載の構造体。

【請求項２０】　1以上の共用サブネットワークの識別子を前記コンピュータシステムによって読取るための手段を更に含む前記構造体において、前記グループの何れか1つにおける各共用サブネットワークと他の任意のサブネットワークとの間でトラフィックが許可され、

1以上の前記ACLによって、前記グループの何れか1つにおける前記共用サブネットワークの何れか1つと任意のサブネットワークとの間でトラフィックが許可されることを特徴とする請求項１６に記載の構造体。

【請求項２１】　少なくとも1つの前記ドメインが、前記ドメインにおけるトラフィックを制限可能であるような前記構造体であって、

1以上のグループの各々に対して、前記グループ内における許可及び／又は拒否されたトラフィックを識別するための情報を前記コンピュータシステムによって読取るための手段であって、前記情報が、トラフィックの制限において1以上のドメインによって使用されるような読取り手段と、

前記情報による指定に従ってトラフィックを許可及び／又は拒否するように、トラフィックを制限可能な各ドメインを前記コンピュータシステムによって構成するための手段とを更に含むことを特徴とする請求項１６に記載の構造体。

【請求項２２】　所定のグループ内において許可及び／又は拒否されたトラフィックを識別するための情報が、1以上の（１）トラフィックを制限可能なドメイン内のトラフィックを各々送信する1以上のスイッチのポートであって、前記グループ内のトラフィックを運ぶための前記1以上のポートと、（２）前記グループに属するエンティティの物理的アドレスと、更に（３）前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項２１に記載の構造体。

【請求項２３】　各サブネットワークの識別子が、アドレス又はアドレスレンジであることを特徴とする請求項１６に記載の構造体。

【請求項２４】　前記1以上の装置が、IPアドレスに基づきトラフィックの経路を指定し、また各ドメイン内において、トラフィックが物理的アドレスに基づき端末間で送信されることを特徴とする請求項１６に記載の構造体。

【請求項２５】　複数のドメインを含む所定のネットワークにおける接続を確立するための方法において、少なくとも1つのドメインが、前記ドメインにおいて規定されたサブドメインを有することができ、前記ドメインによって、単一のサブドメイン内のトラフィックが許可されるが、サブドメイン間のトラフィックが拒否され、更に、

各グループ内においてトラフィックが許可されるように1以上の接続グループを規定する過程であって、少なくとも1つの接続グループに対して、コンピュータシステムに前記接続グループに属するトラフィックを規定する情報を与えるよ

うな前記規定過程と、

少なくとも1つの接続グループに対して、前記コンピュータシステムに前記接続グループのメンバであるサブドメインの識別子を与える過程と、

少なくとも1つの接続グループに対して、前記サブドメインによって前記接続グループにおけるトラフィックが許可されるように、前記コンピュータシステムが、前記接続グループにおけるサブドメインを有する各ドメインを構成する過程とを含むことを特徴とする方法。

【請求項２６】　トラフィックを規定する前記情報が、少なくとも1つのグループに対して、1以上の（１）単一のドメイン内のトラフィックを各々送信する1以上のスイッチのポートであって、前記グループ内のトラフィックを運ぶための1以上の前記ポートと、（２）前記グループのメンバである端末の物理的アドレスと、更に（３）前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項２５に記載の方法。

【請求項２７】　各々のドメインを構成する過程が、前記グループにおけるサブドメインを有する単一のドメイン内のトラフィックを送信するスイッチについて、（ａ）前記グループのメンバである端末の物理的アドレス間のトラフィックを許可するための、また（ｂ）異なるグループのメンバである端末の物理的アドレス間のトラフィックを拒否するための前記スイッチを構成する過程を含むことを特徴とする請求項２６に記載の方法。

【請求項２８】　複数のドメインを含む所定のネットワークにおける接続を確立するための構造体において、少なくとも1つのドメインが、前記ドメインにおいて規定されたサブドメインを有することが可能であり、前記ドメインによって、単一のサブドメイン内のトラフィックが許可されるが、サブドメイン間のトラフィックが拒否され、更に、

1以上の接続グループのセットにおける各接続グループに属するトラフィックを規定する情報をコンピュータシステムによって受信するための手段であって、トラフィックが各グループ内で許可されるような前記受信手段と、

少なくとも1つの接続グループについて、前記接続グループのメンバであるサブドメインの識別子を前記コンピュータシステムによって受信する手段と、

少なくとも1つの接続グループについて、前記サブドメインによって前記接続グループにおけるトラフィックが許可されるように、前記接続グループにおいてサブドメインを有する各ドメインを前記コンピュータシステムによって構成するための手段とを含むことを特徴とする所定の構造体。

【請求項２９】　トラフィックを規定する前記情報が、少なくとも1つのグループに対して、1以上の（１）単一のドメイン内のトラフィックを各々送信する1以上のスイッチのポートであって、前記グループ内のトラフィックを運ぶための1以上の前記ポートと、（２）前記グループのメンバである端末の物理的アドレスと、更に（３）前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項２８に記載の構造体。

【請求項３０】　前記構造体が、前記コンピュータシステム及び該コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステムと前記プログラムとの組合せが、前記全ての手段を含むことを特徴とする請求項２８に記載の構造体。

【請求項３１】　前記全ての手段を実施するための命令を含むコンピュータの読取り可能媒体であることを特徴とする請求項２８に記載の構造体。

【請求項３２】　各ドメイン内のトラフィックが、端末の物理的アドレスに基づき端末間で送信され、またドメイン間のトラフィックが、端末の論理的アドレスに基づき経路指定されることを特徴とする請求項２８に記載の構造体。

【発明の詳細な説明】

【０００１】

発明の背景

本発明はネットワークに関連するもので、また詳細にはネットワークにおける接続性の確立に係るものである。

【０００２】

セキュリティ上の理由やネットワークの通信量を低減する目的で、幾つかのネットワークでは接続を制限している。従って、ネットワークにおける幾つかの端末が互いに通信を許可される一方で、別の端末は通信を許可されない。接続は、通信を許可された端末間の物理的な通信リンクが確立されることによって可能となるか、或いは通信を許可されていない端末間の物理的な通信リンクが確立されないことによって禁止され得る。しかし、これは各セットの接続の制限のための物理的リンクを個別に構成することが必要であるので実際的ではない。従って、コマンドを発行してネットワーク装置を割当てることによってネットワークの接続性を確立する或いは変更するための技術が発達してきた。

【０００３】

これについて図１及び図２に示す（これらの図には先行技術にはない本発明の幾つかの態様が示してある）。ネットワーク１１０は、大規模な組織の相互接続に適する企業ネットワークである。ネットワーク１１０には、「第2層ドメイン(layer 2 domains)」１１６Ｐ、１１６Ｑ、１１６Ｒ、１１６Ｓ、１１６Ｔが含まれる（用語「第2層」は、D. Bierersらの”NetWare:4 for Professionals”(1993)、1-9頁（ここで言及することにより本明細書の一部とする）に記載のOSI参照モデルのを指す）。同一の第2層ドメイン１１６に属する端末１２４（例えば、ドメイン１１６Ｐにおける端末124.1、124.2）は、それらのMACアドレス（「第2層」アドレス）を用いて互いに通信可能である。MAC（媒体アクセス制御）アドレスは、端末のネットワークインタフェースカード（NIC）に書込まれた物理的アドレスであるか、又はNICスイッチの設定によって確立された物理的アドレスである。全てのドメイン１１６又はその幾つかには、1以上のネットワークスイッチ（NICスイッチと混同しない）が含まれ得る。各ドメイン１１６のスイッチ１２８は

、端末のMACアドレスを用いて端末１２４間でトラフィックを送信する。

【０００４】

異なる第2層ドメインにおける端末（例えば、端末124.1、124.3）は、MACアドレスのみを使用して互いに通信することはできない。それらは、論理アドレスであるIPアドレスを用いて通信する。ルータ130.1、130.2、130.3は、端末のIPアドレス（必要に応じてIPアドレスとMACアドレスとの間で変換される）に基づきドメイン１１６間のトラフィックの経路を指定する。

【０００５】

幾つかのドメイン１１６においては、バーチャルLAN（即ち、VLAN）を用いて接続性を制限することができる。例えば、ドメイン１１６Ｐには3つのVLAN １４０ａ、１４０ｂ、１４０ｃが含まれる（図２）。ドメイン１１６Ｐにおける端末１２４は、それらが同一のVLANに属している場合にのみ、第2層において（即ち、それらの第2層アドレスを用いて）互いに通信可能である。従って、図１に示すVLAN１４０ａに属する端末124.1、124.2は通信可能である。

【０００６】

VLANは、LANスイッチ１２８によって実現される。詳述すると、スイッチ１２８は、同一のVLAN内の端末間のみでパケットを送信する。（スイッチ１２８は、VLANへのトラフィックを制限可能なので、「VLAN－capable」と称される。例えば、ドメイン１１６Ｓ、１１６Ｔのような幾つかの第2層ドメインには、非VLAN－capableスイッチが含まれ得る。）

異なる第2層ドメイン間の接続は、ルータ１３０によって制限される。ルータ１３０は、IPアドレスに基づき接続の制限を規定するアクセス制御リスト（ACLs）を使用する（例えば、K．Siyan及びC．Hareの" Internet Firewalls and Network Security"（1995），187-192頁を参照）。

【０００７】

アクセス制御リストの作成及びVLANの規定は、ネットワーク管理者を混乱させる面倒なプロセスであり得る。このプロセスは、動的ネットワーク環境においては度々繰返されねばならず、そこでは端末、ユーザ、及びネットワークサービスが或る場所から別の場所へ移動し、又は物理的な移動なしに或る組織から他の組

織へ移され、或いは付加もしくは除去される。

【０００８】

従って、ネットワークにおける接続の設定を容易にすることが望ましい。

【０００９】

発明の開示

本発明は、ネットワークの接続を確立及び制約するための新しい方法とシステムを提供するものである。幾つかの実施例においては、VLAN及びアクセス制御リストの容易な生成が可能となる。

【００１０】

幾つかの実施例においては、アクセス制御リストが管理端末(management station)によって作成される。管理端末は接続グループの規定を受信する。各接続グループ(connectivity groups)はサブネットワークのグループである。トラフィックは各グループの中で許可される。幾つかの実施例において、各サブネットワークはIPサブネットとして識別される。管理端末は、接続グループを規定する情報からアクセス制御リストを作成する。

【００１１】

幾つかの実施例において、管理端末は共用サブネットワークの識別子を受信し、また任意の接続グループにおける任意のサブネットワークと共用サブネットワークとの間のトラフィックを許可するACLを生成する。

【００１２】

幾つかの実施例において、管理端末は、例えばVLANのようなサブドメインを、ドメインを適切に構成することによって生成する。ネットワーク管理者は、ドメインを構成するためにそのグループに属するトラフィックを規定する各接続グループ情報に入力する。そのような情報の例には、同一の接続グループに属するエンティティ（例えば、スイッチのポート、ネットワーク端末のMACアドレス、又はログオン時にユーザによって指定されるユーザ名）のリストが含まれる。異なる接続グループからのエンティティは通信を許可されない。接続グループは、異なる第2層ドメインからのエンティティを含み得る。エンティティは、どのエンティティがどのVLANに属するかを指定することなしに、接続グループに対して割

当てられ得る。管理端末は、同一のグループにおける何れのエンティティが所定の単一のドメインに属するかを決定し、そのようなエンティティを適切なVLANに配置する。

【００１３】

幾つかの実施例において、接続グループにおけるトラフィックを規定する情報には、第2層パケットのビットの値が含まれる。

【００１４】

本発明は、第2層ドメイン、スイッチ、又はルータに限られるものではない。本発明の他の特徴及び優位性については後述する。本発明は添付した請求の範囲で規定されるものである。

【００１５】

発明の詳細な説明

ネットワーク１１０には、5つの第2層ドメイン１１６が含まれる。各ドメインにおけるパケットのアドレス指定が、OSI参照モデルの第2層（データリンク層）におけるパケットの内容に基づき行われるので、これらのドメインは「第2層」と称される。ルータ１３０は、第3層（ネットワーク層）におけるパケットの内容に基づきトラフィックの経路を指定する。特に、IPアドレスは、第3層のアドレスである。しかし、本発明は第2層若しくは第3層又はOSI参照モデルに従うネットワークに限定されるものではない。

【００１６】

ドメイン１１６Ｐには、MACアドレスに基づきトラフィックを送信するVLAN－capableスイッチ128.1、128.2が含まれる。それらのスイッチは、トランク150.1によって互いに接続されている。各スイッチは、ネットワークセグメントに各々接続されている1以上のポートを有する。従って、スイッチ128.1のポート160.1は、端末124.1を含むネットワークセグメントに接続されている。また、スイッチ128.2のポート160.2は、端末124.2を含むネットワークセグメントに接続されている。図１において、各ネットワークセグメントは単一の端末を含む。或る実施例においては、ネットワークセグメントは複数の端末を含む。

【００１７】

スイッチ128.1のポート１６０Ｍは、後述するような接続グループの生成に用いられる管理端末１２４Ｍに接続される。

【００１８】

スイッチ128.1は、トランク150.2によってルータ130.1に接続される。ルータ130.1は、ルータ130.2、130.3、及びインターネット１７０に接続される。ルータ130.2は、ルータ130.3に接続される。ルータ130.2は、トランク150.3によってドメイン１１６ＱのVLAN－capableスイッチ128.3に接続される。ドメイン１１６Ｑには、VLAN－capableスイッチ128.4、128.5、及び128.6が含まれ、その各々はスイッチ128.1、128.2と同様に1以上のネットワークセグメントに接続される。ここでは、端末124.3を含むセグメントのみ示す。また、ドメイン１１６Ｑのスイッチ１２８は互いに接続されている。

【００１９】

ルータ130.2は、第2層ドメイン１１６Ｔに接続されている。

【００２０】

ルータ130.3は、ドメイン１１６ＲのVLAN－capableスイッチ128.7及び第2層ドメイン１１６Ｓに接続されている。スイッチ128.7は、スイッチ128.1、128.2と同様にネットワークセグメント（図示せず）に接続されている。ドメイン１１６Ｓ、１１６Ｔはスイッチを全く含まないか、或いは幾つかのスイッチ（図示せず）を含む。

【００２１】

幾つかの実施例において、1以上のドメイン１１６はスイッチを全く含まないか、或いは非VLAN－capableスイッチ、ハブ又はコンセントレータ含む。

【００２２】

前述のように、異なるドメイン間の通信にはIPアドレスが使用される。例えば、端末124.3にパケットを送信するために、端末124.1は、端末124.3のIPアドレス及びルータ130.1のMACアドレスを、それぞれ論理的宛先アドレス及び物理的宛先アドレスとしてパケットに書込む。ルータ130.1は、宛先MACアドレスをルータ130.2のMACアドレスと置き換え、端末124.1の発信元MACアドレスをルータ130.1のMACアドレスに置き換える。次にルータ130.1が、パケットをルータ130.2に送

信する。ルータ130.2は、パケットの発信元MACアドレスを自身のMACアドレスに置き換え、また宛先MACアドレスを端末124.3のMACアドレスに置き換えて、パケットをスイッチ128.3に送信する。スイッチ128.3は、パケットをスイッチ128.5経由で端末124.3に送信する。ドメイン１１６Ｐには重複していないVLAN１４０ａ、１４０ｂ、１４０ｃ（図２）が含まれ、ドメイン１１６Ｑには、重複していないVLAN１４０ｄ、１４０ｅ、１４０ｆが含まれ、ドメイン１１６Ｒには重複していないVLAN１４０ｇ、１４０ｈ、１４０ｉが含まれる。VLANにおける端末のメンバーシップは、端末が接続されているスイッチポート１６０によって規定されるか、端末のMACアドレスによって規定されるか、或いは端末にログオンしたユーザのユーザ名によって規定される。ポート又はMACアドレスに基づくVLANのメンバーシップの確定については、G. Heldの“Virtual LANs: Construction, Implementation, and Management”（1997），233-249頁（ここで言及することにより本明細書の一部とする）に開示されている。

【００２３】

ユーザ名によるVLANのメンバーシップの確定については、付録Ａに記載されている（“User-Based Binding of Network Stations to Broadcast Domains”と題するJ. Ekstromらの米国特許出願08/832,011（1997年4月2日出願；ここで言及することにより本明細書の一部とする）を参照）。或る実施例においては、VLAN１４０が，ポートによって識別される端末、MACアドレスによって識別される端末、及び／又はユーザ名によって識別される端末を結び付ける。

【００２４】

ドメイン１１６Ｓ、１１６Ｔは、任意のVLANを含む場合もあり、また含まない場合もある。

【００２５】

管理端末１２４Ｍは、VLAN１４０ｂに属する。端末１２４Ｍは、任意のスイッチ１２８及び任意のルータ１３０と通信可能である。或る実施例において、（１）全てのスイッチ１２８は、Cisco社（San Jose, California）から入手可能なtype Catalyst® のスイッチであり、また（２）ルータ１３０は、Cisco社から入手可能なルータであり、それらはCisco社の説明書に記載されている（部品番号7

8-2040-01）。これらは、ここで言及することにより本明細書の一部とする。

【００２６】

ネットワーク１１０には、種々のドメイン１１６におけるエンティティ（非トランクスイッチポート１６０、MACアドレス、又はユーザ名）を含む接続グループが含まれる。例えば、接続グループは、VLAN１４０ａ、１４０ｄ、１４０ｇにおける全てのエンティティによって構成され得る。通信は、同一の接続グループにおけるエンティティ間においては許可され、異なる接続グループにおけるエンティティ間においては拒否される。詳述すると、スイッチ１２８及びルータ１３０は、或る接続グループにおける端末１２４から別の接続グループにおける端末１２４へのパケットの経路は指定しない。

【００２７】

周知のように、VLANは同報通信ドメインである（また、ここでは「第2層同報通信ドメイン」又は「第2層 BD」と称される）。対照的に、接続グループは必ずしも同報通信ドメインではない。従って、幾つかの実施例においては、同報通信又はマルチキャストトラフィックは単一のVLANに制限される。

【００２８】

また、本明細書においてVLANは「バーチャル同報通信ドメイン」即ちVBDと称される。VBDは、ネットワークにおいて必ずしも物理的な接続（例えば、ケーブル）の変更の必要なしに規定され得る同報通信ドメインである。

【００２９】

管理端末１２４Ｍには、プログラムやデータを記憶するための記憶装置１９２、並びにキーボード、スクリーン、及び／又は他のインタフェース機器のようなユーザインタフェース機器１９４が含まれる。

【００３０】

付録Ｂは、幾つかの実施例における接続グループを生成する（特に、VLAN１４０及びルータアクセス制御リストを生成する）プロセスを示している。ここで、このプロセスは図１のVLANの例に示してあり、また3つの接続グループは以下の通りである。

【００３１】

グループ１は、VLAN１４０ａ、１４０ｄ、及び１４０ｇからなる。

【００３２】

グループ２は、VLAN１４０ｂ、１４０ｅ、及び１４０ｈからなる。（このグループは、管理端末１２４Ｍを含む管理接続グループとして指定され得る。）

グループ３は、VLAN１４０ｃ、１４０ｆ、及び１４０ｉからなる。

【００３３】

幾つかの実施例においては、第2層ドメイン１１６Ｓは同報通信ドメインである。付録Ｂのプロセスは、ドメイン１１６Ｓを、任意の接続グループとの通信を許可された共用IPサブネットとして構成する。重要なことは、各第2層同報通信ドメインが、IPサブネット又はIPサブネットの組合せであることである。

【００３４】

付録Ｂのプロセスは、第2層ドメイン１１６Ｔ及び関連するサブネットを「非管理(unmanaged)」状態にする（即ち、対応するルータインタフェースに対してACLが生成されず、更にプロセスによって生成された任意のACLにおいてサブネット１１６Ｔは明示されない。）。従って、ドメイン１１６Ｔは任意の接続グループからトラフィックを受取り可能であるが、ドメイン１１６Ｔから任意の接続グループへのトラフィックは、ルータ１３０によって取除かれ得る（遮断され得る）。

【００３５】

幾つかの実施例において、単一の第2層ドメインには、管理されたサブネット及び非管理のサブネットが含まれる。

【００３６】

付録Ｂのプロセスは、任意のVLAN又は接続グループがネットワーク１１０において確立される前か或いは確立された後に実施され得る。幾つかの実施例において、付録Ｂプロセスが最初に実施され、全てのドメイン１１６（場合によって、ドメイン１１６Ｓ、１１６Ｔのような共用ドメイン及び非管理のドメインのエンティティを除く）における全ての通信エンティティを含む単一の「管理接続グループ(management connectivity group)」を確立する。その管理グループによっ

て、管理端末１２４Ｍが全てのスイッチ及びルータと通信可能となる。次に付録Ｂプロセス又は付録Ｇのメンテナンスプロセスが実施され、前述のグループ１、２、３又は別の任意のグループを確立する。そのようなグループの設置は、管理端末がスイッチ及びルータと通信する能力によって容易となる。

【００３７】

或いは、管理端末１２４Ｍ及びスイッチ１２８のポートのみが管理接続グループに配置される。幾つかの実施例においては、スイッチ１２８のそれらのポートのみが管理接続グループに配置され、その管理接続グループは管理端末１２４Ｍを全てのVLAN－capableスイッチ及び全てのルータと通信可能とすることを要求される。

【００３８】

後述する実施例においては、付録Ｂプロセスの開始時に接続グループが存在しないと仮定する。

【００３９】

付録Ｂのプロセスが開始される前に、各ルータ１３０が構成されて、1以上のIPサブネットが各ルータインタフェース２１０に割当てられる（図２）。（Cisco社の説明書において「サブインタフェース」と称される幾つかに対して、ここでは用語「インタフェース」を用いることに注意されたい。）付録Ｂのプロセスが完了した後に、各ルータ１３０は、それらが接続されるドメイン１１６の各VLAN１４０に対して個別のインタフェースを有し得る。

【００４０】

各VLAN１４０はサブネット又はサブネットの組合せであるので、経路指定ソフトウェアがVLANを明確に認識しない場合でも、ルータ１３０がVLANに基づき事実上の送信決定を行うことに注意されたい。ルータは、ルータのトランクポート（例えば、トランクポート２２０）経由でドメインに接続され、また各インタフェースはトランクポートの論理的サブポートである。

【００４１】

周知の通り、ルータ及びスイッチのトランクポート（即ち、スイッチ、又はスイッチ及びルータと相互接続するトランク１５０に接続されたポート）は、マル

チプルVLANのためのトラフィックを運ぶ。トランクポートにおけるトラフィックはトランクプロトコル(trunking protocol)を使用し、そこで各パケットは、パケットが割当てられるVLANの識別子を標識したより大きなパケットにカプセル化(encapsulated)される。VLANメンバーシップがMACアドレスよりも寧ろポートによって規定される場合、VLANの標識によって受信スイッチ１２８がパケットのVLANを識別することが可能となる。

【００４２】

ルータ１３０はトランクプロトコルを理解し、同一のトランクポートにおける種々のVLANからのトラフィックを、各VLANからのトラフィックがVLANに割当てられた個別のポートに到達した場合のように取り扱う。

【００４３】

幾つかの実施例においては、トランクの代わりにルータと第2層ドメインとの間の個別の物理的接続を用いて個々のVLANに対するトラフィックを運ぶ。

【００４４】

各インタフェースは、インタフェースによって取扱われる各サブネットにおけるゲートウェイアドレスを有する。ゲートウェイアドレスは、サブネットにおけるルータのアドレスである。

【００４５】

付録Ｃは、記憶装置１９２において付録Ｂの幾つかのステップによって作成されたデータベースを示す。

【００４６】

ステップＭ５（付録Ｂ）において、ネットワーク管理者は、管理端末１２４Ｍにネットワーク１１０のIPアドレスレンジを与える。付録Ｂの例において、アドレスレンジは10.0.0.0/8である。ネットワーク１１０において、各サブネットは255.255.255.0のサブネットマスクを有する。

【００４７】

IPアドレスレンジ及びサブネットは、形式10.0.0.0/8（サブネットマスクは、全て0が続く有意な8つの1を有する）を有するか、或いはIPアドレス（10.0.0.0）及びネットマスク（255.0.0.0）の組合せのような形式を有する。

【００４８】

付録ＣのＩ１に示すように、管理端末１２４ＭはネットワークＩＩＯのIPアドレスレンジをそのデータベースに入力する。

【００４９】

付録Ｂに示すように、ステップＭ７が管理者によって実施される。端末１２４Ｍがデータ構造Ｉ２を生成する（付録Ｃ）。この情報及び付録Ｃにおける他の情報は、異なる実施例においては異なって編成される。例えば、幾つかの実施例において、項目Ｉ２－１（スイッチのアドレス）は、各ドメインに対するアドレスのリストとして格納される。別の実施例においては、同様の情報は、アドレス及び各ドメインのペアとして格納される。別の実施例においては他のデータ構造が用いられる。

【００５０】

ステップＭＩＯにおいて、ネットワーク管理者がVLANＩ４０を規定する。VLANの規定には、各ドメインＩＩ６における各スイッチＩ２８及び端末１２４Ｍに対してVLAN識別子を与える過程が含まれる。VLAN識別子は、スイッチＩ２８に認識可能な識別子（即ち、VLAN番号）である。例えば、スイッチ128.1、128.2の各々は、VLANＩ４０ａ、１４０ｂ、１４０ｃの識別子を受信し、スイッチ128.7は、VLANＩ４０ｇ、１４０ｈ、１４０ｉの識別子を受信する。VLANを規定する過程には、何れのエンティティ（ポート、MACアドレス又はユーザ名）が各々のVLANに属するかを明らかにする過程は含まれない。

【００５１】

或る実施例においては、管理者がVLAN識別子を各スイッチＩ２８に直接入力する。別の実施例においては、管理者がVLAN識別子を各ドメインＩＩ６の制御スイッチＩ２８に入力する。制御スイッチは、同一のドメインにおける別のスイッチ（仮に存在すれば）に対して識別子を送信する。更に別の実施例においては、管理者はこの情報を例えばTelnet又はSNMPプロトコルを用いて端末１２４Ｍから遠隔のスイッチＩ２８に情報を与える。

【００５２】

付録ＣのＩ３に示すように、端末１２４Ｍはこの情報をそのデータベースに格

納する。

【００５３】

ステップＭ１４において、ネットワーク管理者は情報１４（付録Ｃ）を端末１２４Ｍに入力する。図１及び図２において、個々のサブネットは各第2層 BDに割当てられ、第2層 BDとIPサブネットとの間に1対1対応が存在する。サブネットは、図２及び次の表１に示されている。

【００５４】

【表１】

表１

第2層BD	サブネット
140a	10.1.1.0/24
140b	10.1.2.0/24
140c	10.1.3.0/24
140d	10.2.1.0/24
140e	10.2.2.0/24
140f	10.2.3.0/24
140g	10.3.1.0/24
140h	10.3.2.0/24
140i	10.3.3.0/24
116S	10.3.4.0/24
116T	10.2.4.0/24

【００５５】

幾つかの実施例においては、複数のサブネットが第2層BDに対して割当てられている。

【００５６】

サブネットは、サブネットマスクの表記法、又はサブネットアドレス及びマスクの表記法における1のサブネットアドレス／番号を用いて端末１２４Ｍに与えられる。

【００５７】

またステップＭ１４において、対応するIPサブネットからの各VLANにおけるIPアドレスを割当てるためにネットワーク１１０が構築される。従って、幾つかのWindows NT™の実施例において、DHCPサーバは各サブネットにおいてIPアドレスを割当てるために構成される。（Windows NTについては、例えばR．Sant'Angeloらの"Windows ｎ NT Server Survival Guide"（1996)に記載されており、これについては、ここで言及することにより本明細書の一部とする。）幾つかの実施例においては、DHCPサーバがルータ１３０においてサブネットの1つに接続される。ルータは、DHCPのリクエストをルータに直接接続された全てのサブネットからこのDHCPサーバへ送信するように構成される。別の実施例においては、個別のDHCPサーバが各サブネットに設けられる。

【００５８】

ステップＭ２０において、各接続グループに対して、管理者は接続グループのメンバであるIPサブネット（即ち、接続グループのメンバである第2層 BDの一部であるIPサブネット）を端末１２４Ｍに入力する。従って、管理者は、接続グループ1に対してVLAN１４０ａ、１４０ｄ、１４０ｇにおけるサブネットを入力し、グループ2に対してVLAN１４０ｂ、１４０ｅ、１４０ｈにおけるサブネットを入力し、更にグループ3に対してVLAN１４０ｃ、１４０ｆ、１４０ｉにおけるサブネットを入力する。或いは、各接続グループに対して、管理者は、接続グループの第2層 BDメンバの識別子を入力する。各々のケースにおいて、全てのルータを管理端末１２４Ｍから到達可能とするために、管理者は、管理接続グループのメンバであるIPサブネットを入力し得る。幾つかの実施例において、各ルータは、共有サブネット又は管理接続グループのサブネットメンバにおける少なくとも1つのゲートウェイIPアドレスを有する。

【００５９】

幾つかの実施例では、全てのルータが管理端末から到達可能であることを必要としない。従って、管理されていないサブネット及び他のルータにのみ直接接続されたルータは、幾つかの実施例においては到達可能であることを必要としない。

【００６０】

項目１５（付録Ｃ）が、ステップＭ２０において生成される。

【００６１】

多数のサブネットが単一の第2層 BDに割当てられた場合，それらは全て同じ接続グループに割当てられる。

【００６２】

ステップＭ３０において、管理者が各接続グループに属するエンティティを端末１２４Ｍに入力する。ここで、１６（付録Ｃ）が生成される。例えば、接続グループ１の場合、管理者はスイッチポート160.1、160.2、160.3（ポート160.3に接続された端末124.3はVLAN１４０ｄに属すると仮定する）、及び他のポート、MACアドレス、並びに／又はVLAN１４０ａ、１４０ｄ、１４０ｇに属するユーザ名を入力する。幾つかの実施例においては、管理者は、ポート、MACアドレス又はユーザ名がどのドメイン又はVLANに属するかを記憶する必要がない。

【００６３】

ポート１６０は、参照が容易なように管理者によって割付けられ得るラベルによって、端末１２４Ｍにおいて識別される。例えば、ポートがユーザ名Fredのユーザによって使用される端末１２４に接続されている場合、管理者はそのポートにラベル「Fred」を割付けることができ、またステップＭ３０において「Fred」を入力してこのポートを接続グループに割付けることが可能である。MACアドレスの接続グループへの割付も同様である。

【００６４】

ステップＭ４０において、管理者は情報１７及び１８（付録Ｃ）を管理端末１２４Ｍに入力する。

【００６５】

ステップＭ４５において、端末１２４MがVLAN１４０を生成し、付録Ｄに示すように各エンティティを適当なVLANに配置する。付録Ｄにおいて、括弧内の番号は、付録Ｄの対応するステップにおいて用いられる付録Ｃのデータベース項目を指す。

【００６６】

付録Ｄにおいて、接続グループのエンティティＥがVLAN－capableスイッチ（ステップＶ１）のポート１６０である場合、そのエンティティはポートが属するドメイン１１６のVLANにのみ配置される。対照的に、エンティティがMACアドレス（ステップＶ２）又はユーザ名（ステップＶ３）である場合、そのエンティティは接続グループの全てのVLANに配置される。MACアドレスの場合では、これによってMACアドレスを有する端末が、その接続グループのVLANを含む任意のドメイン１１６に接続され得る。従って、接続グループ1におけるMACアドレスを有する携帯用コンピュータ（例えば、ラップトップコンピュータ）は、ドメイン１１６Ｐ、１１６Ｑ、１１６Ｒに接続され得る。コンピュータがドメイン１１６Ｐに接続される場合、発信元アドレスとしてコンピュータのMACアドレスを有するパケットを受信するスイッチ128.1、128.2によって、コンピュータがVLAN１４０ａに配置され得る。同様に、例えばコンピュータがドメイン１１６Ｑに接続される場合、それはVLAN１４０ｄに配置され得る。

【００６７】

同様に、ユーザ名が接続グループの全てのVLAN１４０に配置される。ユーザがドメイン１１６Ｐにログオンした場合、ユーザを適切なVLANに切替えるためにUBNCサーバに対する要求がドメイン１１６Ｐから届く。例えばユーザ名が接続グループ1に存在する場合、UBNCサーバはユーザをVLAN１４０ａに配置する。同様に、ユーザがドメイン１１６Ｑ又は１１６Ｒにログオンする場合、UBNCサーバは、ユーザをVLAN１４０ｄ又は１４０ｇにそれぞれ配置する。

【００６８】

ステップＶ３において、「実施例１」は接続グループに関連する任意の事項を知るためにUBNCサーバを必要としない。端末１２４Ｍは、各ドメイン１１６におけるユーザ名に対してどのVLANが割当てられるかをUBNCサーバに知らせる（ステップＶ３－２）。実施例２においては、UBNCサーバはどのVLANがどの接続グループに属するかを認識している（この情報はUBNCサーバに直接与えられるか、或いは例えば端末１２４Ｍから遠隔的に与えられ得る）。従って、実施例２のステップＶ３－１において、端末１２４ＭはどのVLANがユーザに割当てられるかをUBNCサーバに通知しない。ユーザがログオンした時、UBNCサーバはログオンが生じた

ドメイン１１６及びユーザの接続グループからユーザのVLANを決定する。UBNCデータベースには、各ドメイン１１６における各VLANに関連するIPサブネットが含まれるので、ドメイン１１６はユーザのIPアドレスから決定される。幾つかの実施例においては、UBNCサーバは管理端末１２４Ｍにおいて作動する。

【００６９】

ステップＭ５０（付録Ｂ）において、端末１２４Ｍは、付録Ｅにおけるプログラムを実行することによって、ルータアクセス制御リストを作成する。個別のアクセス制御リストが、接続グループのサブネット番号が直接結び付けられる各ルータインタフェースに対して作成される。付録Ｅのプログラムは、ルータ130.2からVLAN１４０ｅまでのインタフェース２１０の例において説明され得る。

【００７０】

各ルータインタフェースに対して、対応するサブネットが所定の接続グループに属する場合、付録Ｆに示すようにステップＡ１からＡ５によってアクセス制御リストが作成される。付録Ｆにおける回線番号（例えば、ＡＬ１－１）は、付録Ｅのステップ番号に対応する。従って、例えばステップＡ１（付録Ｅ）は回線ＡＬ１－１を生成し、ステップＡ２は回線ＡＬ１－２ａ及びＡＬ１－２ｂを生成する。

【００７１】

付録Ｆは、Cisco社（San Jose, California）の幾つかのルータによって用いられるシンタクスを用いる。このシンタクスについては、K. Siyan及びC. Hareの"Internet Firewalls and Network Security"（1995），186-191頁に記載されており、これについてはここで言及することにより本明細書の一部とする。回線番号（例えばＡＬ１－１）は、アクセス制御リストの一部ではない。更に、感嘆符「！」で始まり行の終わりまで続く文章は、ルータによって無視されるコメントである。これらのコメントは幾つかの実施例においては省略される。

【００７２】

ステップＡ１は、サブネット１１６Ｓのような各共用サブネットからのインタフェース２１０へのトラフィックを許可する回線を生成する。そのプログラムは、アクセス制御リストに対して、「アクセスリスト(access-list)」、アクセス

制御リスト番号（幾つかの実施例においてプログラム自身によって連続的に発生する）、「許可 ip（permit ip）」、共用サブネットのIPアドレス、並びに0.0.0.255のワイルドカードマスクを書き込む。（入力のパケットIPと比較して、ワイルドカードマスクにおける0ビットは、発信元IPアドレスの対応するビットがルータによって使用されていることを示し、ワイルドカードマスクにおける1ビットは、対応するビットが使用されていないことを示す。）

回線ＡＬ１－１におけるワイルドカードマスク0.0.0.255は、サブネットマスクを反転させることによって決定される。

【００７３】

ステップＡ２は、同一の接続グループにおける他の全てのサブネット（即ち、第2層 BD）からのトラフィックを許容する例えば回線ＡＬ１－２ａ、ＡＬ１－２ｂのような回線を生成する。回線ＡＬ１－２ａは、サブネット10.1.2.0/24（VLAN１４０ｂ）からのトラフィックを許容する。回線ＡＬ１－２ｂは、サブネット10.3.2.0/24（VLAN１４０ｈ）からのトラフィックを許容する。

【００７４】

ステップＡ３は、ネットワーク１１０における他の全ての端末からのトラフィックを拒否する回線ＡＬ１－３を生成する。（重要なことは、ルータがパケットを受取ったときに、ルータがアクセス制御リストの始めからパケットの開始をテストすることである。パケットに適合する行が発見されたとき、アクセス制御リストの残りの部分は無視される。）ワイルドカードマスクは、ネットワーク１１０のIPアドレスレンジマスクを反転させることによって得られる。

【００７５】

ステップＡ４によって、インターネット１７０からのトラフィックを含むネットワーク１１０の外部の任意の端末からのトラフィックを許容する回線ＡＬ１－４が生成される。

【００７６】

幾つかの実施例において、管理者は、ステップＭ５０の前に接続グループにおける各サブネットに対して、インターネットからサブネットへのトラフィックが許可されるかどうかを管理端末１２４Ｍに示す。トラフィックが拒否された場合

は、対応するインタフェースに対してステップＡ４が省略され、またステップＡ３がラインＡＬ１－３の代わりの「任意の拒否ip (deny ip any)」回線を生成する。

【００７７】

付録Ｅに示すようにステップＡ５が実施される。

【００７８】

ルータインタフェースが接続グループのBDメンバに接続されずに、共用若しくは非管理サブネット（例えば１６０Ｓ）又はインターネット１７０に接続される場合、ACLは生成されずにサブネット若しくはインターネットは他の任意のサブネットからアクセス可能となる。

【００７９】

幾つかの実施例においては、付録ＢのステップＭ４０において、管理者は各共用サブネットに対してどのようなアクセスが与えられるかを指定し、付録Ｅのプロセスによって、当業者に周知の方法を用いて適切なアクセス制御リストが作成される。例えば、共用サブネットがネットワーク１１０の中からのみアクセス可能とされる場合、アクセス制御リストは以下のように構成され得る。

【００８０】

アクセスリスト１許可ip　10.0.0.0　0.255.255.255

アクセスリスト１拒否ip　任意

別の実施例において、そのような機能性は、ルータ130.1又は他の幾つかの機器（図示せず）において具現される企業全体に広がるファイアウォールによって与えられる。

【００８１】

管理端末１２４Ｍは、存在する全てのアクセス制御リストを消去して、新しいアクセス制御リストに置き換えるように各ルータ１３０に指示する。

【００８２】

幾つかの実施例においては、ネットワーク管理者は追加のコマンドをアクセス制御リストに挿入することが可能である。従って、幾つかの実施例においては、管理者が、ステップＭ５０の前に対応するインタフェースに対してアクセス制御

リストに挿入される各サブネットの追加項を指定し得る。詳述すると、管理者は、ステップＡ１の前に挿入される項、ステップＡ２とＡ３の間で挿入される項、ステップＡ３とＡ４の間で挿入される項、及びステップＡ４の後に挿入される項を指定することができる。幾つかの実施例において、この技術を用いてファイアウォールの機能をアクセス制御リストに組込み、従って、企業全体に渡る個別のファイアウォールの必要はなくなる。

【００８３】

幾つかの実施例においては、ステップＭ１０及びＭ２０が省略される。ステップＭ４５において、各接続グループに対して、管理端末１２４Ｍは、VLAN―capableスイッチ及び接続グループにおける1以上のエンティティを有する各ドメイン１１６においてVLANを生成し、またVLANにエンティティを配置する。（従って、ドメインが接続グループにおけるポート１６０を有する場合、或いは接続グループにMACアドレス又はユーザ名が含まれる場合に、VLANがドメインの中に生成される。）また端末１２４Ｍによって、IPサブネット（例えば、10.1.1.0/24）が、VLANに割当てられる。

【００８４】

幾つかの実施例においては、VLANのメンバーシップは、ポート、MACアドレス又はユーザ名以外の他の基準によって決定される。従って、幾つかの実施例においては、VLANのメンバーシップは、例えば第2層パケットにおける所定のビットの値のようなパケットの内容に基づき決定される。スイッチ１２８が、1以上の値の予め決定されたセットの中にそのようなビットの値が存在するパケットを受取るとき、そのスイッチは、パケットの発信元MACアドレス、又はパケットが到達するポート１６０を対応するVLANに配置する。スイッチ１２８がルータに接続されたトランクポートにおけるパケットを送信する場合、スイッチはパケットにパケットのVLAN番号を付加する。ルータ１３０において、各VLAN番号はインタフェースに関連するものである。（この関係は、インタフェースが規定されたときに確立される。）従って、図2に示すように、各ルータ１３０は、そのルータが直接接続される各IPサブネットに対する個別のインタフェース２１０を有する。付録Ｂ～Ｇの実施例と同様に接続グループが生成される。特にステップＭ３０に

おいて、管理者は、各接続グループに対して、どのようなパケットがその接続グループに属するかを決定するルールを指定する。例えば、所定のルールによって所定のビットの値を有するパケットが所定の接続グループに属することが決定され得る。

【００８５】

幾つかの実施例においては、ルータ１３０におけるアクセス制御リストによって、IPアドレスとは別の基準に基づきトラフィックを許可するか或いは拒否する。例えば、或る基準にはポート番号が関係する（例えば、W. Cheswick及びS. Bellovinの“Firewalls and Internet Security”（1994），94-109頁を参照；ここで言及することにより本明細書の一部とする）。更に、所定の基準によって、インタフェースへのトラフィックよりも寧ろインタフェースからのトラフィックを指定する。管理者は、ステップＭ５０の前に端末１２４Ｍに対して十分な情報を与え、そのような基準に従ってアクセス制御リストを作成する。

【００８６】

幾つかの実施例においては、冗長(redundancy)を目的として、VLAN１４０が同一のルータの異なるインタフェース２１０に接続され得る。2つのインタフェースは、同一のサブネットか或いは2つの異なるサブネットに割当てられる。各ACLは、両方のインタフェースに対して同様の制限を与える。

【００８７】

VLANが種々のルータのインタフェースに接続されるとき、場合によっては別のルータからアクセス可能な別の端末への情報の経路を指定するために、ルータの1つがVLANを経由して別のルータへデータを送信することを試みることができる。その場合、VLANに接続されたインタフェースに対するACLが、ルータ間のトラフィックを過度に制限しないように構築される。

幾つかの実施例においては、VLANサブネットは共用されるか或いは非管理であり、任意の接続グループのメンバではない。

【００８８】

付録Ｇは、ネットワーク１１０において接続性を変更するためのメンテナンスプロセスを示す。付録Ｂのプロセスの再実行によって、任意の変更を行うことが

可能である。しかしながら、幾つかの実施例において付録Ｇプロセスがメンテナンスを容易にする。

【００８９】

幾つかの実施例において、ステップＭ５０は省略される（ACLは生じない）。

【００９０】

前述の実施例は本発明を限定するものではない。本発明は、特定のネットワーク、層、スイッチ、ルータ、オペレーティングシステム、或いは他のハードウェア若しくはソフトウェアに限定されるものではない。また本発明は企業ネットワークに限定されるものではない。幾つかの実施例においては、MACアドレスはNICに書込まれるものではなく、ソフトウェアによって生じる。幾つかの実施例において、付録Ｂ－Ｇの管理ソフトウェアの全て或いはその一部は端末１２４より遠スイッチ１２８又はルータ１３０で実行される。ソフトウェアは幾つかの実施例に適用される。

【００９１】

幾つかの実施例においては、ドメイン１１６は第2層プロトコルとは別のプロトコルを使用し、ルータ１３０は、第3層プロトコルとは別のプロトコルに基づきトラフィックの経路指定を行う。各ドメインにおける接続性は、MACアドレス又は第2層パケットの内容とは別の情報に基づき決定され、ルータ１３０は、IPアドレスとは別の情報に基づきトラフィックを許容又は拒否する。幾つかの実施例においては、ルータ１３０はIPXアドレスを使用する。幾つかの実施例においては、D. Bierer らの "NetWare® 4 for Professionals" (1993)（ここで言及することにより本明細書の一部とする）に記載のネットウェア若しくはアップルトークネットワークを使用する。他の実施例及び変更例は、添付した請求の範囲によって規定される本発明の範囲内である。

付録Ａ

ユーザベースネットワークコントロール（UBNC）

幾つかの実施例において、VLANのメンバーシップは端末にログオンしたユーザに基づき決定される。Windows NT™ の幾つかの実施例においては、UBNCサーバが全てのVLANからアクセス可能なように設置される（例えば、サーバが共用サブネ

ット内にある）。ネットワーク端末が能力アップされた(powered up)とき、それは「デフォルト(default)」VLANに配置される（デフォルトVLANは各々の第2層ドメイン１１６に存在する）。端末は、デフォルトVLANを提供するDHCPサーバからIPアドレスを受取る。ユーザが端末にログオンした時、端末はUBNCサーバに対して、ログオン時に与えられたユーザ名に関連するVLANに端末を切替えるように要求を送る。その要求には、ユーザ名、端末のMACアドレス、及び端末の現在のIPアドレスが含まれる。UBNCサーバは、UBNCサーバデータベースから関連するVLANを決定する。或る実施例においては、各ユーザ名に対して、データベースには関連するVLANの識別子が含まれる。別の実施例においては、データベースには管理端末によって与えられる以下のような情報が含まれる。

【００９２】

（Ａ）各ユーザ名について、そのユーザ名が属する接続グループの識別子

（Ｂ）各接続グループに属するVLANの識別子

（Ｃ）各VLANについて、関連するサブネット

UBNCサーバが要求を受取ると、サーバは要求する端末に対して（１）端末が異なるVLANに切替えられるかどうかの指示（端末がデフォルトVLANにないときにユーザがログオンした場合、切替が要求されない可能性があり、またVLANが規定されていないレイヤ2 BDにユーザがログオンした場合、切替が行われない可能性がある。）、並びに（２）ユーザに割当てられたVLANのIPサブネット及びサブネットマスクを送信する。次にUBNCサーバは、端末がそのDHCPリース(DHCP lease)を解放するのを待つ。そこでUBNCサーバは、端末を含む第2層ドメイン１１６における単一のスイッチ又は複数のスイッチ１２８に対して適切なコマンドを送信する。そのスイッチによって、ユーザに割当てられたVLANに端末が配置される。

【００９３】

UBNCサーバからの応答を受取った後に、端末はそのDHCPリースを解放し、次にサーバが端末を割当てられたVLANに切替え可能なように所定の期間待つ。その期間の後に、端末は切替が完了したと想定し、新たなDHCPリースの要求を送出する。応答において、端末は新たなIPアドレスを受取る。端末は新たなIPをUBNCサーバから受取ったサブネットマスク及びIPサブネットと照合する。新たなIPがサブ

ネットに存在しない場合、端末は新たな要求をUBNCサーバに対して送出することによってその手続きを繰り返す。端末が新たなIPを要求したときに端末が割当てられたVLANに切替えられていない場合、新たなIPは間違ったサブネットに存在する可能性がある。

【００９４】

幾つかの実施例においては、デフォルトVLANは省略される。別の実施例においては、全ての端末又は地理的にもっとも近い端末のグループが個別のデフォルトVLANに割当てられ、UBNCサーバによってユーザがそれらと関連するVLANに切替えられるまで通信を制限する。ユーザがログオフした時、ユーザ端末は適切なデフォルトVLANに戻される。

付録Ｂ

接続グループ(Connectivity Groups)の生成

Ｍ５　管理端末１２４Ｍにネットワーク１１０のIPアドレスレンジ（例えば、10.0.0.0/8）を与える。

Ｍ７　管理端末１２４Ｍに情報Ｉ２（付録Ｃ）を与える。

Ｍ１０　VLANを定義する。

Ｍ１４　第2層 BDにIPサブネットを割当てる。

Ｍ２０　各接続グループに対して、管理端末にグループのIPサブネットメンバを与える。1つの接続グループを管理接続グループとして指定する。

Ｍ３０　接続グループに管理可能なエンティティ（ポート、MACアドレス及び／又はユーザ名）を割当てる。

Ｍ４０　管理端末に情報Ｉ７及びＩ８を与える

Ｍ４５　管理端末１２４Ｍが、エンティティを適切なVLANに配置する（付録Ｄ参照）。

Ｍ５０　管理端末１２４Ｍが、ルータのためのアクセス制御リストを作成する（付録Ｅ参照）。

付録Ｃ

管理端末データベース

Ｉ１　ネットワーク１１０のIPアドレスレンジ

Ｉ２　各ドメイン１１６について

Ｉ２－１　ドメイン１１６における全てのVLAN－capableスイッチ１２８のIPアドレス

Ｉ２－２　各スイッチの非トランクポート１６０の識別子

Ｉ３　各ドメイン１１６について、ドメインにおけるVLANの識別子

Ｉ４　各第2層 BDについて、BDがVLANであるか否か、またIPサブネットがBDに含まれているか否かの指示。BDがVLANである場合、VLANの識別子。

Ｉ５　各接続グループについて、その接続グループに属するIPサブネット

Ｉ６　各接続グループについて、その接続グループに属するエンティティ（ポート、MACアドレス、及び／又はユーザ名）

Ｉ７　各ルータインタフェースについて

Ｉ７－１　関連するサブネット（仮に存在すれば）

Ｉ７－２　インタフェースがVLAN－capable第2層ドメインに接続されているか否かを指示するフラッグ

Ｉ８　ネットワーク１１０における全ての共用サブネットのリスト

付録D

VLANの生成

各接続グループCGについて、また接続グループにおける各エンティティＥ（Ｉ６）について、

Ｖ１　エンティティＥがVLAN－capableスイッチ１２８のポート１６０である場合、

Ｖ１－１　ポートが属するドメイン１１６－Ｅ（１１６Ｐ、１１６Ｑ、１１６Ｒの1つ）を検索する（Ｉ２－２、Ｉ２－１）

Ｖ１－２　接続グループCG及びドメイン１１６－Ｅの両方におけるVLANを検索する（Ｉ３、Ｉ４、Ｉ５）

Ｖ１－３　ドメイン１１６－Ｅのスイッチ１２８又はドメイン１１６－Ｅの制御スイッチ１２８に対してコマンドを送信することによってポートＥをVLANに配置する

Ｖ２　或いはエンティティＥがMACアドレスである場合、接続グループCGにおけ

る各VLANについて（Ｉ４、Ｉ５）、

Ｖ２－１　VLANを含むドメイン１１６－Ｖ（１１６Ｔ、１１６Ｑ、１１６Ｒの1つ）を決定する（Ｉ３）

Ｖ２－２　ドメイン１１６－Ｖの制御スイッチ１２８又は全てのスイッチ１２８に対して適切なコマンドを送信することによってMACアドレスＥ５VLANに配置する

Ｖ３　或いはエンティティＥがユーザ名である場合、

実施例１：接続グループCGにおける各VLANについて（Ｉ４、Ｉ５）、

Ｖ３－１　VLAN（Ｉ３）を含むドメイン１１６－Ｖを決定する

Ｖ３－２　VLAN識別子、ドメイン１１６－Ｖの識別子、及びユーザ名をUBNCサーバに対して送信する

実施例２：

Ｖ３－１　接続グループCGの識別子及びユーザ名をUBNCサーバに送信する

付録Ｅ

ステップＭ５０：リクエストに対するアクセス制御リストの生成

ネットワーク１１０における各ルータについて（Ｉ２－３）、またルータの各インタフェースについて（Ｉ７）、インタフェースと接続されたサブネットが接続グループに属する場合、

Ａ１　各共用サブネットからのトラフィックを許可する（Ｉ８）

Ａ２　同一の接続グループにおける全ての別のサブネットからのトラフィックを許可する（Ｉ５、Ｉ４）

Ａ３　ネットワーク１１０における他の全ての別のサブネットからのトラフィックを拒否する（Ｉ１）

Ａ４　ネットワーク１１０の外部からのトラフィックを許可する

Ａ５　ルータにおいてTelnetセッションを開放し、ルータに対して以下を送信する

（１）インタフェースから存在するACL（もし存在すれば）を取除くためのコマンド（例えば、非アクセスグループ１）

（２）アクセスリスト

（３）コマンド：

interface vlan_e

access-group 1 out

これらのコマンドにより、ACLが「vlan_e」と標識されたルータインタフェースに対して割当てられる

付録Ｅ

VLAN１４０ｅに対するルータインタフェース２１０のためのアクセス制御リスト

ＡＬ１―１　アクセスリスト1許可ip　10.3.4.0　0.0.0.255

！共用サブネット

ＡＬ１―２ａ　アクセスリスト1許可ip　10.1.2.0　0.0.0.255

！同一のものにおけるサブネット

！企業の接続グループ

ＡＬ１―２ｂ　アクセスリスト1許可ip　10.3.2.0　0.0.0.255

！同一のものにおけるサブネット

！企業接続グループ

ＡＬ１―３　アクセスリスト1拒否ip　10.0.0.0　0.255.255.255

！ネットワーク１１０における全てのサブネット

！同一の接続グループの外部

ＡＬ１―４　アクセスリスト1許可ip　任意

！へからのアクセスの許可

！ネットワーク１１０の外部

付録Ｇ

メンテナンスアルゴリズム

非管理から接続グループのメンバへのサブネットの変更

サブネットが1以上のゲートウェイアドレスを有する場合、サブネットは接続グループのメンバに変更されない。さもなければ、サブネットを接続グループに付加し、付録Ｅに示すように、同一の接続グループにおけるサブネットが直接接続される各々のインタフェースに対するアクセス制御リストを再生成する。

非管理から共用へのサブネットの変更

共用サブネットのリスト１８（付録Ｃ）にサブネットを付加する。付録Ｅに示すように、任意の接続グループにおけるサブネットが接続される各ルータインタフェースのアクセス制御リストを再生成する。（サブネットは各ACLに付加され得る。）

共用から非管理へのサブネットの変更

共用サブネットのリスト１８（付録Ｃ）からサブネットを除去する。付録Ｅに示すように、任意の接続グループにおけるサブネットが接続される各ルータインタフェースのアクセス制御リストを再生成する。（サブネットは各ACLから除去され得る。）

共用から接続グループのメンバへのサブネットの変更

サブネットが１を越えるゲートウェイアドレスを有する場合、サブネットは接続グループのメンバに変更されない。さもなければ、サブネットを共用サブネット（付録Ｃ）のリスト１８から除去し、またサブネットを接続グループ（付録Ｃにおける１４）に付加する。付録Ｅに示すように、任意の接続グループにおけるサブネットが接続される各ルータインタフェースのアクセス制御リストを再生成する。

接続グループのメンバから非管理へのサブネットの変更

接続グループ（付録Ｃの１５）からサブネットを除去する。付録Ｅに示すように、同一の接続グループにおけるサブネットが直接接続される各ルータのインタフェースのアクセス制御リストを再生成する。（サブネットは各ACLから除去され得る。）付録Ｅに示すように、サブネットは直接接続されたルータインタフェースに対するACLを除去し、次に（必要ならば）再生成する。（インタフェースに直接接続された他のサブネットが存在しない場合は、ACLは生成されない。別の単一のサブネット又は複数のサブネットが存在する場合は、適切なACLが生成される。）

接続グループのメンバから共用へのサブネットの変更

接続グループ（付録Ｃにおける１５）からサブネットを除去する。サブネットが直接接続されているルータインタフェースに対するACLを除去する。付録Ｅに示すように、任意の接続グループにおけるサブネットが直接接続されている各ル

ータインタフェースのアクセス制御リストを再生成する。（サブネットは、グループのメンバとして幾つかのACLから取除かれるが、共用サブネットとして各ACLに付加される。）

1つの接続グループ（「旧」グループ）から別のグループ（「新」グループ）へのサブネットの移行

サブネットを旧グループから取除き、新グループ（付録Ｃの１５）に付加する。付録Ｅに示すように、古い又は新規の接続グループの何れかにおけるサブネットが直接接続された各ルータインタフェースのACLを再生成する。

接続グループへの通信エンティティ（ポート、MACアドレス、ユーザ等）の付加（ステップＭ３０参照）

管理者は、新しいエンティティが属すべき接続グループを指示する。

【００９５】

ポート１６０　ポートはスイッチ１２８に接続され、それはそれ自体が第2層ドメイン１１６の一部である。所定の第2層ドメインにおいて、選択された接続グループは特定のサブネットと接続され、それは、それ自体が特定のVLANと結ばれる。ポートが接続グループに割付けられる際に、ステップＶ１（付録Ｄ）が実行され、ポートが第2層ドメインにおける接続グループのメンバであるVLANに配置される。マルチポイントモジュールがスイッチに付加される場合のように、或いは全部のスイッチがネットワークに付加される場合のように、通常はポートがグループに付加されることに注目されたい。これらの場合において、新しいポートの全てのセットが、管理者によって選択された接続グループに付加される。次に（もし必要ならば）管理者は1つずつポートの割当を変更することができる。

【００９６】

MACアドレス　ポートに関する場合のように、特定の第2層ドメインにおいて、選択された接続グループがサブネット／VLANペアに接続される。各第2層ドメインに対して、ステップＶ２（付録Ｄ）によって、所定のMACアドレスが指定されたVLANに割当てられるように、全てのスイッチ（又はスイッチの能力次第で、単一の制御スイッチ）が形成される。

【００９７】

ユーザ　付録Ｄのステップ Ｖ３を参照。

或る接続グループ（「旧」グループ）から別のグループ（「新」グループ）への通信エンティティ（ポート、MACアドレス、ユーザ）の移行（ステップＭ３０参照）

ポート１６０　ポートはVLAN－capableスイッチ１２８に接続され、それはそれ自体が第2層ドメインの一部である。第2層ドメインにおいて、新旧の接続グループは特定のサブネットに接続され、それらは、それら自体が特定のVLANに結ばれる。（新しい接続グループに属する第2層ドメインにおいてサブネットが存在しない場合、変更は行われない。）管理端末１２４Ｍは、新しいVLANに対するポートのVLANの割当を変更する。

【００９８】

MACアドレス　ポートの場合のように、特定の第2層ドメインにおいて、新規の接続グループはサブネット／VLANペアに関連する。各第2層ドメインについて、所定のMACアドレスが指定されたVLANに割当てられるように、端末１２４Ｍが全てのスイッチ（又はスイッチの能力次第で、単一の制御スイッチ）を構成する。特定の第2層ドメインにおける要求された接続グループに対応するサブネットが存在しない場合、第2層ドメインにおけるMACアドレスに対するVLANの割当は行われない。移行の結果として、或いは第2層ドメインにプラグインされたラップトップ又は他のモバイルコンピュータにMACアドレスが割当てられるために、MACアドレスが第2層ドメインに生じた場合、そこでスイッチは未知のMACアドレスが発生したときに、それらが通常とり得る全ての動作をとり得る。

【００９９】

ユーザ　付録Ｄのステップ Ｖ３を参照。

新規のルータインタフェース／VLAN／サブネットの付加

新規のルータインタフェース２１０が、直接接続されたサブネットを含まない場合（ゲートウェイアドレスがない場合）、動作は要求されない。さもなければ、インタフェースは1以上のゲートウェイアドレス及び対応する直接接続されたサブネットを有する。直接接続された各サブネットについて、

１．サブネットが既に接続グループのメンバである（従って、別のルータのイ

ンタフェースに直接接続されている）場合、サブネットは共用サブネットに変更される。前述の接続グループのメンバから共用サブネットへサブネットを変更するためのプロセスを参照されたい。

【０１００】

２、或いはサブネットが共用又は非管理として既に指定されている場合、動作は要求されない。

【０１０１】

３、或いはサブネットは新規のサブネットである。サブネットを共用サブネットのリスト１８（付録Ｃ）に付加する。付録Ｅに示すように、任意の接続グループにおけるサブネットが直接接続された各ルータインタフェースのアクセス制御リストを再生成する。（サブネットは共用サブネットとして各ACLに付加され得る。）サブネットがVLAN－capableスイッチ１２８を含む第2層ドメインに存在する場合、新規のVLANがドメインの中に生成され、新規のサブネットと接続される。

新規のルータの付加

新規のルータ１３０は幾つかのインタフェースを有し得る。各ルータインタフェースに対して、新規のルータインタフェースのためにリストされた動作が実行される。

新規のVLAN－capableスイッチの付加

新規のVLAN－capableスイッチ１２８が第2層ドメインに付加され、そこでは管理接続グループに割当てられたサブネットが存在し、またこのグループに対応するVLANが存在する。

【０１０２】

スイッチが、ポートベースVLAN(port-based VLANs)を具現する場合、スイッチの管理スタック及びスイッチにおける全てのポートは、管理接続グループにおけるサブネットに対応するVLANに割当てられる。更に、スイッチはこのサブネットからのIPアドレスに割当てられる。例えば、サブネット10.50.3.0/24が、管理グループに割当てられた第2層ドメインにおけるサブネットである場合、またVLAN３が、サブネット10.50.3.0/24に関連するVLANである場合、管理接続グループに

おけるアドレスに割当てるために、Cisco Catalyst 5000シリーズスイッチのコンソールにおいて次のようにコマンドを発行する。

【０１０３】

set interface sc0 3 10.50.3.200 255.255.255.0 10.50.3.255

ここでsc0は、スイッチの管理スタックに対する指名子であり、3は、サブネット10.50.3.0/24に対応するVLANであり、10.50.3.200は、スイッチの管理スタックに割当てられたサブネット10.50.3.200/24におけるIPアドレスであり、255.255.255.0は、サブネット10.50.3.0/24に対するサブネットマスクであり、更に10.50.3.255は同報通信アドレスである。

【０１０４】

スイッチがMACアドレスベースVLANを具現する場合、管理スタックのMACアドレスは、管理接続グループにおけるサブネットに対応するVLANに割当てられる。ポートベースVLANの場合のように、スイッチはこのサブネットからのIPアドレスに割当てられる。

新規の接続グループの付加

新規の（空の）接続グループは常に付加され得る。サブネットを接続グループにどのように付加するかについては前述の通りである。

【図面の簡単な説明】

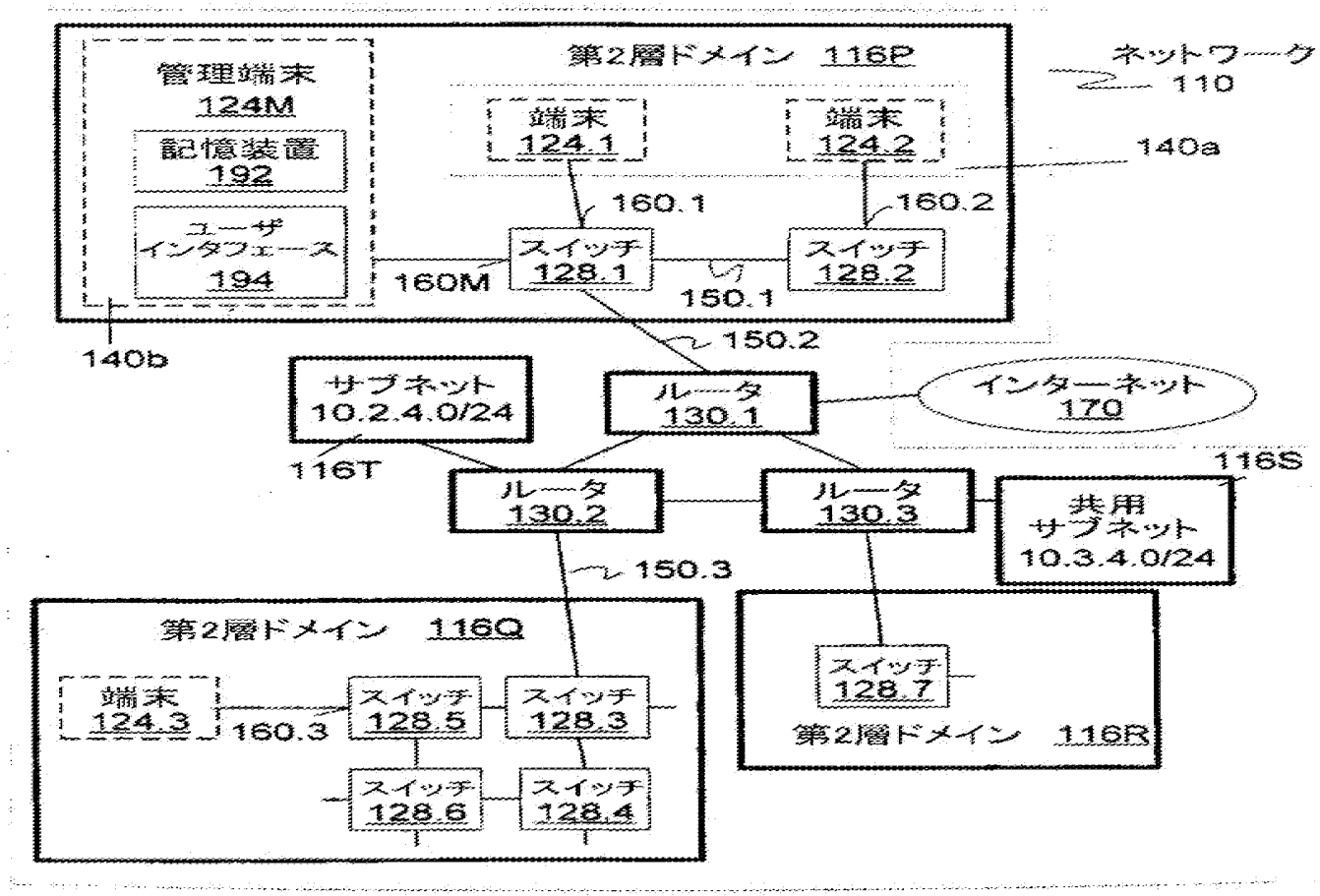
【図１】

本発明により接続を確立したネットワークのブロック線図である。

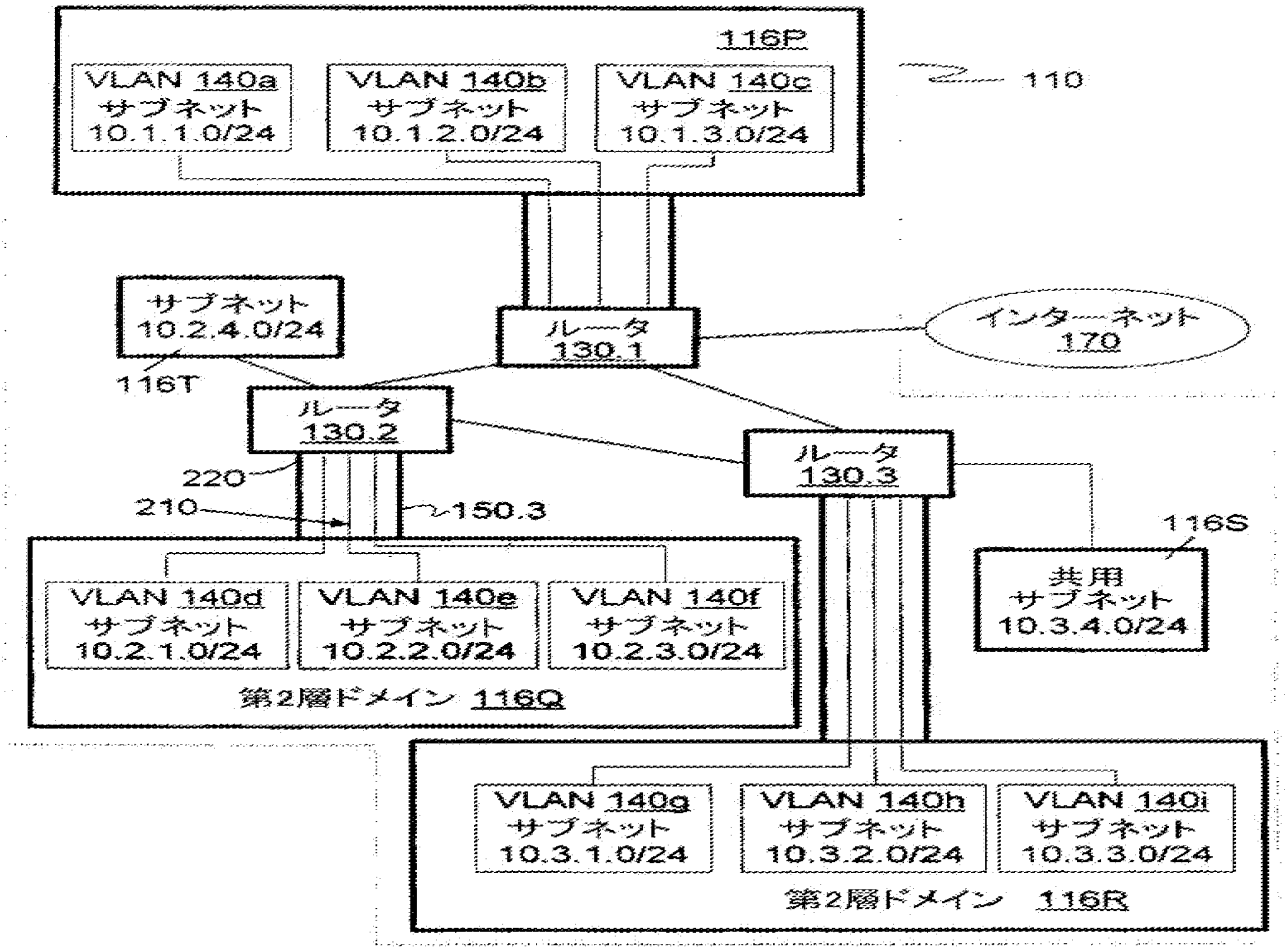
【図２】

図１のネットワークにおけるVLAN及びルータインタフェースを示すブロック線図である。

【図１】


管理端末
124M
記憶装置
192
ユーザ
インタフェース
194
140b
第2層ドメイン 116P
端末
124.1
端末
124.2
140a
160.1
160.2
スイッチ
128.1
スイッチ
128.2
160M
150.1
150.2
ネットワーク
110
サブネット
10.2.4.0/24
116T
ルータ
130.1
インターネット
170
ルータ
130.2
ルータ
130.3
116S
共用
サブネット
10.3.4.0/24
150.3
第2層ドメイン 116Q
端末
124.3
160.3
スイッチ
128.5
スイッチ
128.3
スイッチ
128.6
スイッチ
128.4
スイッチ
128.7
第2層ドメイン 116R

【図２】


116P
VLAN 140a
サブネット
10.1.1.0/24
VLAN 140b
サブネット
10.1.2.0/24
VLAN 140c
サブネット
10.1.3.0/24
110
サブネット
10.2.4.0/24
116T
ルータ
130.1
インターネット
170
ルータ
130.2
ルータ
130.3
220
210
150.3
116S
共用
サブネット
10.3.4.0/24
VLAN 140d
サブネット
10.2.1.0/24
VLAN 140e
サブネット
10.2.2.0/24
VLAN 140f
サブネット
10.2.3.0/24
第2層ドメイン 116Q
VLAN 140g
サブネット
10.3.1.0/24
VLAN 140h
サブネット
10.3.2.0/24
VLAN 140i
サブネット
10.3.3.0/24
第2層ドメイン 116R

【手続補正書】特許協力条約第３４条補正の翻訳文提出書
【提出日】平成１２年４月１２日（２０００．４．１２）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　ネットワーク端末をバーチャル同報通信ドメイン（VBDs：１４０ａ乃至１４０ｉ）に接続するための方法であって、
ネットワーク上においてネットワーク端末のユーザを識別する情報を前記ネットワーク端末から受信する過程と、
ユーザを識別する情報から1以上のVBDを含むユーザの属する接続グループを決定する過程と、
前記ネットワーク端末が接続される1以上のVBDを決定する過程であって、前記1以上のVBDが前記接続グループのメンバであるような前記決定過程と、
前記ネットワーク端末を前記1以上のVBDに接続するためのコマンドを発行する過程とを含むことを特徴とする方法。
【請求項２】　各VBDが、前記トラフィックが生じる前記VBDへの同報通信トラフィックを制限可能なドメイン（１１６Ｐ）のサブドメインであり、
前記接続グループが、少なくとも2つのドメインからのVBDを含み、
前記ネットワーク端末が接続された1以上のVBDが、前記ネットワーク端末を含む前記ドメインに基づき決定されることを特徴とする請求項１に記載の方法。
【請求項３】　各VBDがVLANであり、また前記ネットワーク端末が、前記接続グループに属するVLAN並びに前記ネットワーク端末を含む前記ドメインに接続されることを特徴とする請求項２に記載の方法。
【請求項４】　ネットワーク端末をバーチャル同報通信ドメイン（VBDs：１４０）に接続するための構造体であって、
ネットワーク上においてネットワーク端末のユーザを識別する情報を前記ネッ

トワーク端末から受信する手段と、

ユーザを識別する情報から1以上のVBDを含むユーザの属する接続グループを決定する手段と、

前記ネットワーク端末が接続される1以上のVBDを決定する手段であって、前記1以上のVBDが前記接続グループのメンバであるような前記決定手段と、

前記ネットワーク端末を前記1以上のVBDに接続するためのコマンドを発行する手段とを含むことを特徴とする構造体。

【請求項５】　各VBDが、前記トラフィックが生じる前記VBDへの同報通信トラフィックを制限可能なドメイン（１１６Ｐ）のサブドメインであり、

前記接続グループが、少なくとも2つのドメインからのVBDを含み、

前記ネットワーク端末が接続された1以上のVBDが、前記ネットワーク端末を含む前記ドメインに基づき決定されることを特徴とする請求項４に記載の構造体。

【請求項６】　各VBDがVLANであり、また前記ネットワーク端末が、前記接続グループに属するVLAN並びに前記ネットワーク端末を含む前記ドメインに接続されることを特徴とする請求項５に記載の構造体。

【請求項７】　前記構造体が、（１）所定のコンピュータシステム（１２４Ｍ）、及び（２）前記コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステム及び前記プログラムが、前記決定手段の各々を含むことを特徴とする請求項４に記載の構造体。

【請求項８】　前記構造体が、所定のコンピュータの読取り可能な媒体であり、そこで各手段が、1以上のコンピュータの命令、コンピュータの読取り可能なデータ、又は1以上の命令及びデータの組合せを含むことを特徴とする請求項４に記載の構造体。

【請求項９】　ネットワークドメイン（１１６Ｐ、１１６Ｑ、１１６Ｒ、１１６Ｓ、１１６Ｔ）間のトラフィックの経路を指定する1以上の装置（１３０）に対して1以上のアクセス制御リスト（ACLs）を生成するための方法において、そのような装置にACLが与えられた場合に、前記装置が、前記ACLを用いて前記ドメイン間においてどのようなトラフィックが許可及び／又は拒否されるかを決定し、更に、

サブネットワークの各グループ内においてトラフィックが許可されるように、サブネットワーク（１４０ａ、１１６Ｔ）の1以上のグループを規定する過程であって、各サブネットワークがネットワークドメインの一部であるか、或いはネットワークドメインの全てであり、また各グループに対して、所定のコンピュータシステムに前記グループに属するサブネットワークの識別子を与えるような前記過程と、

前記コンピュータシステムが、各グループ内のトラフィックを許可するために1以上のACLを生成する過程とを含むことを特徴とする方法。

【請求項１０】　前記1以上のACLが異なるグループにおけるサブネットワーク間のトラフィックを拒否する前記複数のグループを規定する過程を含むことを特徴とする請求項９に記載の方法。

【請求項１１】　1以上の共用サブネットワークの識別子を受信する前記コンピュータシステムを更に含む前記方法において、トラフィックが、前記グループの何れか1つにおける各共用ネットワークと任意の別のサブネットワークの間において許可され、

1以上のACLによって、トラフィックが、前記グループの何れか1つにおける前記共用サブネットワークの何れか1つと任意のサブネットワークとの間において許可されることを特徴とする請求項９に記載の方法。

【請求項１２】　少なくとも1つの前記ドメインが、前記ドメインにおけるトラフィックを制限することが可能であるような前記方法であって、

1以上のグループの各々に対して、前記コンピュータシステムが、前記グループ内において許可及び／又は拒否されたトラフィックを識別するための情報を受信する過程であって、前記情報が、制限するトラフィックにおける1以上のドメインによって使用されるような前記受信過程と、

前記情報による指定に従ってトラフィックを許可及び／又は拒否するように、前記コンピュータシステムがトラフィックを制限可能な各ドメインを構成する過程とを更に含むことを特徴とする請求項９に記載の方法。

【請求項１３】　所定のグループ内において許可及び／又は拒否されたトラフィックを識別するための情報が、1以上の（１）トラフィックを制限可能な

ドメイン内のトラフィックを各々送信する1以上のスイッチ（１２８）のポート（１６０）であって、前記グループ内のトラフィックを運ぶための前記ポート（１６０）と、（２）前記グループに属するエンティティ（１２４）の物理的アドレスと、更に（３）前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項１２に記載の方法。

【請求項１４】　各サブネットワークの識別子が、アドレス又はアドレスレンジであることを特徴とする請求項９に記載の方法。

【請求項１５】　前記1以上の装置が、IPアドレスに基づきトラフィックの経路を指定し、また各ドメイン内において、トラフィックが物理的アドレスに基づき端末間で送信されることを特徴とする請求項９に記載の方法。

【請求項１６】　ネットワークドメイン（１１６Ｐ、１１６Ｑ、１１６Ｒ、１１６Ｓ、１１６Ｔ）間のトラフィックの経路を指定する1以上の装置（１３０）に対して1以上のアクセス制御リスト（ACLs）を生成するための所定の構造体において、そのような装置にACLが与えられた場合に、前記装置が、前記ACLを用いて前記ドメイン間においてどのようなトラフィックが許可及び／又は拒否されるかを決定し、更に、

各グループ内においてトラフィックが許可されるように、サブネットワーク（１４０、１１６）の1以上のグループをコンピュータシステムに対して規定する手段であって、各サブネットワークがネットワークドメインの一部であるか、或いはネットワークドメインの全てであり、また各グループに対して、前記グループに属するサブネットワークの識別子をコンピュータシステムによって読取るための前記規定手段と、

前記コンピュータシステムによって、各グループ内のトラフィックを許可するために1以上のACLを生成するための手段とを含むことを特徴とする構造体。

【請求項１７】　前記構造体が、前記コンピュータシステム（１２４Ｍ）及び該コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステムと前記プログラムとの組合せが、前記規定手段及び生成手段を含むことを特徴とする請求項１６に記載の構造体。

【請求項１８】　前記構造体が、前記規定手段及び前記生成手段を実施す

るための命令を含むコンピュータの読取り可能媒体であることを特徴とする請求項１６に記載の構造体。

【請求項１９】　前記規定手段が複数のグループを規定するときに、前記1以上のACLが異なるグループにおけるサブネットワーク間のトラフィックを拒否することを特徴とする請求項１６に記載の構造体。

【請求項２０】　1以上の共用サブネットワーク（１１６Ｓ）の識別子を前記コンピュータシステムによって読取るための手段を更に含む前記構造体において、前記グループの何れか1つにおける各共用サブネットワークと他の任意のサブネットワークとの間でトラフィックが許可され、

1以上の前記ACLによって、前記グループの何れか1つにおける前記共用サブネットワークの何れか1つと任意のサブネットワークとの間でトラフィックが許可されることを特徴とする請求項１６に記載の構造体。

【請求項２１】　少なくとも1つの前記ドメインが、前記ドメインにおけるトラフィックを制限可能であるような前記構造体であって、

1以上のグループの各々に対して、前記グループ内における許可及び／又は拒否されたトラフィックを識別するための情報を前記コンピュータシステムによって読取るための手段であって、前記情報が、トラフィックの制限において1以上のドメインによって使用されるような読取り手段と、

前記情報による指定に従ってトラフィックを許可及び／又は拒否するように、トラフィックを制限可能な各ドメインを前記コンピュータシステムによって構成するための手段とを更に含むことを特徴とする請求項１６に記載の構造体。

【請求項２２】　所定のグループ内において許可及び／又は拒否されたトラフィックを識別するための情報が、1以上の（１）トラフィックを制限可能なドメイン内のトラフィックを各々送信する1以上のスイッチ（１２８）のポート（１６０）であって、前記グループ内のトラフィックを運ぶための前記1以上のポート（１６０）と、（２）前記グループに属するエンティティの物理的アドレスと、更に（３）前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項２１に記載の構造体。

【請求項２３】　各サブネットワークの識別子が、アドレス又はアドレス

レンジであることを特徴とする請求項１６に記載の構造体。

【請求項２４】　　前記1以上の装置が、IPアドレスに基づきトラフィックの経路を指定し、また各ドメイン内において、トラフィックが物理的アドレスに基づき端末間で送信されることを特徴とする請求項１６に記載の構造体。

【請求項２５】　　複数のドメイン（１１６）を含む所定のネットワークにおける接続を確立するための方法において、

各ネットワーク端末が、第１の型のアドレス及び第２の型のアドレスを有することが可能であり、

各ドメインにおけるネットワーク端末間のトラフィックが、宛先ネットワーク端末の第２の型のアドレスを用いることなしに、前記宛先ネットワーク端末の第１の型のアドレスを使用して前記宛先ネットワーク端末に送信され、一方でドメイン間においては、前記宛先ネットワーク端末の第２の型のアドレスを使用してトラフィックが送信され、また制限され、

ドメインが単一のサブドメイン内のトラフィックを許可し、一方でサブドメイン間のトラフィックを拒否するように、少なくとも1つのドメインが、前記ドメインにおいて規定されたサブドメイン（１４０）を有することが可能であり、更に、

接続グループＣＧ１に属するトラフィックを規定する情報ＩＮＦ１をコンピュータシステム（１２４Ｍ）に与える過程であって、前記接続グループＣＧ１が、種々のドメインにおいてサブドメインを有するためのものであり、それらの少なくとも2つがサブドメインへのトラフィックをそれぞれ制限可能であるような前記過程と、

少なくとも前記接続グループＣＧ１について、ドメインが、前記第２の型のアドレスを用いることなしに前記第１の型のアドレスを使用してトラフィックを送信するときに、前記ドメインＤ１が前記情報ＩＮＦ１によって規定されたトラフィックを許可し、一方でサブドメインＳＤ１へのそのようなトラフィックを制限するように、前記コンピュータシステムが、前記接続グループＣＧ１におけるサブドメインＳＤ１を有する各ドメインＤ１を生成する過程とを含むことを特徴とする方法。

【請求項２６】　　トラフィックを規定する前記情報が、少なくとも1つのグループに対して、1以上の（１）単一のドメイン内のトラフィックを各々送信する1以上のスイッチ（１２８）のポート（１６０）であって、前記グループ内のトラフィックを運ぶための1以上の前記ポート（１６０）と、（２）前記グループのメンバである端末（１２４）の物理的アドレスと、更に（３）前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項２５に記載の方法。

【請求項２７】　　各々のドメインを構成する過程が、前記グループにおけるサブドメインを有する単一のドメイン内のトラフィックを送信するスイッチについて、（ａ）前記グループのメンバである端末の物理的アドレス間のトラフィックを許可するための、また（ｂ）異なるグループのメンバである端末の物理的アドレス間のトラフィックを拒否するための前記スイッチを構成する過程を含むことを特徴とする請求項２６に記載の方法。

【請求項２８】　　複数のドメイン（１１６）を含む所定のネットワークにおける接続を確立するための構造体において、

各ネットワーク端末が、第１の型のアドレス及び第２の型のアドレスを有することが可能であり、

各ドメインにおけるネットワーク端末間のトラフィックが、宛先ネットワーク端末の第２の型のアドレスを用いることなしに、前記宛先ネットワーク端末の第１の型のアドレスを使用して前記宛先ネットワーク端末に送信され、一方でドメイン間においては、前記宛先ネットワーク端末の第２の型のアドレスを使用してトラフィックが送信され、また制限され、

ドメインが単一のサブドメイン内のトラフィックを許可し、一方でサブドメイン間のトラフィックを拒否するように、少なくとも1つのドメインが、前記ドメインにおいて規定されたサブドメイン（１４０）を有することが可能であり、更に、

接続グループＣＧ１に属するトラフィックを規定する情報ＩＮＦ１をコンピュータシステム（１２４Ｍ）によって受信するための手段であって、前記接続グループＣＧ１が、種々のドメインにおいてサブドメインを有するためのものであり

、それらの少なくとも2つがサブドメインへのトラフィックをそれぞれ制限可能であるような前記受信手段と、

少なくとも1つの接続グループについて、前記接続グループのメンバであるサブドメインの識別子を前記コンピュータシステムによって受信する手段と、

少なくとも前記接続グループＣＧ１について、ドメインが、前記第２の型のアドレスを用いることなしに前記第１の型のアドレスを使用してトラフィックを送信するときに、前記ドメインＤ１が前記情報ＩＮＦ１によって規定されたトラフィックを許可し、一方でサブドメインＳＤ１へのそのようなトラフィックを制限するように、前記接続グループＣＧ１におけるサブドメインＳＤ１を有する各ドメインＤ１を前記コンピュータシステムによって構成するための手段とを有することを特徴とする構造体。

【請求項２９】　トラフィックを規定する前記情報が、少なくとも1つのグループに対して、1以上の（１）単一のドメイン内のトラフィックを各々送信する1以上のスイッチ（１２８）のポート（１６０）であって、前記グループ内のトラフィックを運ぶための1以上の前記ポート（１６０）と、（２）前記グループのメンバである端末（１２４）の物理的アドレスと、更に（３）前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項２８に記載の構造体。

【請求項３０】　前記構造体が、前記コンピュータシステム及び該コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステムと前記プログラムとの組合せが、前記全ての手段を含むことを特徴とする請求項２８に記載の構造体。

【請求項３１】　前記全ての手段を実施するための命令を含むコンピュータの読取り可能媒体であることを特徴とする請求項２８に記載の構造体。

【請求項３２】　各ドメイン内のトラフィックが、端末の物理的アドレスに基づき端末間で送信され、またドメイン間のトラフィックが、端末の論理的アドレスに基づき経路指定されることを特徴とする請求項２８に記載の構造体。

【手続補正２】

【補正対象書類名】明細書

【補正対象項目名】０００３
【補正方法】変更
【補正内容】
【０００３】
これについて図１及び図２に示す（これらの図には先行技術にはない本発明の幾つかの態様が示してある）。ネットワーク１１０は、大規模な組織の相互接続に適する企業ネットワークである。ネットワーク１１０には、「第2層ドメイン(layer 2 domains)」１１６Ｐ、１１６Ｑ、１１６Ｒ、１１６Ｓ、１１６Ｔが含まれる（用語「第2層」は、D. Bierersらの”NetWare:4 for Professionals”(1993), 1-9頁に記載のOSI参照モデルのを指す）。同一の第2層ドメイン１１６に属する端末１２４（例えば、ドメイン１１６Ｐにおける端末124.1, 124.2）は、それらのMACアドレス（「第2層」アドレス）を用いて互いに通信可能である。MAC（媒体アクセス制御）アドレスは、端末のネットワークインタフェースカード（NIC）に書込まれた物理的アドレスであるか、又はNICスイッチの設定によって確立された物理的アドレスである。全てのドメイン１１６又はその幾つかには、1以上のネットワークスイッチ（NICスイッチと混同しない）が含まれ得る。各ドメイン１１６のスイッチ１２８は、端末のMACアドレスを用いて端末１２４間でトラフィックを送信する。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００２３
【補正方法】変更
【補正内容】
【００２３】
ユーザ名によるVLANのメンバーシップの確定については、付録Ａに記載されている。（”User-Based Binding of Network Stations to Broadcast Domains”と題するJ. Ekstromらの米国特許第5,968,126号(1999年10月19日発行)を参照。これについては、ここで言及することにより本明細書の一部とする。）或る実施例においては、VLAN１４０が、ポートによって識別される端末、MACアドレスに

よって識別される端末、及び／又はユーザ名によって識別される端末を結び付ける。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inter... Ional Application No
PC:/US 99/08866

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/45 H04L12/18

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 02821 A (3COM CORP) 22 January 1998 (1998-01-22) abstract page 1, line 25 - page 7, line 20 figures 10,11	1-10,12, 14-19, 21, 23-25, 28,30-32
A		11,26,27
A	EP 0 812 086 A (NIPPON TELEGRAPH & TELEPHONE) 10 December 1997 (1997-12-10) abstract page 2, column 1, line 21 - page 3, column 3, line 34 page 3, column 4, line 50 - page 4, column 5, line 58 figures 1,2,5,7-9	1,4,9, 16,25,26

-/---

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

° Special categories of cited documents :
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 September 1999	15/09/1999
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Poggio, F

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/08866

C (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SAUNDERS S: "SWITCH PUTS VIRTUAL LANS ON AUTOMATIC PILOT. AGILE'S ATMIZER SWITCH IS THE FIRST TO AUTOMATE SETUP OF VIRTUAL WORKGROUPS" DATA COMMUNICATIONS, vol. 23, no. 12, 1 September 1994 (1994-09-01), page 45/46 XP000462380 ISSN: 0363-6399 the whole document	7,8,13, 15,17, 18, 22-24, 26,27, 29-32
A	AXNER D H: "DIFFERING APPROACHES TO VIRTUAL LANS" BUSINESS COMMUNICATIONS REVIEW, December 1993 (1993-12), pages 42-45, XP000659940 abstract	1,4,9, 16,25,28

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 99/08856

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9802821 A	22-01-1998	AU 3728497 A	09-02-1998
		GB 2330285 A	14-04-1999
EP 0812086 A	10-12-1997	JP 10056473 A	24-02-1998

フロントページの続き

(81)指定国　　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＯＡ(ＢＦ，ＢＪ，ＣＦ，ＣＧ，ＣＩ，ＣＭ，ＧＡ，ＧＮ，ＧＷ，ＭＬ，ＭＲ，ＮＥ，ＳＮ，ＴＤ，ＴＧ)，ＡＰ(ＧＨ，ＧＭ，ＫＥ，ＬＳ，ＭＷ，ＳＤ，ＳＬ，ＳＺ，ＵＧ，ＺＷ)，ＥＡ(ＡＭ，ＡＺ，ＢＹ，ＫＧ，ＫＺ，ＭＤ，ＲＵ，ＴＪ，ＴＭ)，ＡＥ，ＡＬ，ＡＭ，ＡＴ，ＡＵ，ＡＺ，ＢＡ，ＢＢ，ＢＧ，ＢＲ，ＢＹ，ＣＡ，ＣＨ，ＣＮ，ＣＵ，ＣＺ，ＤＥ，ＤＫ，ＥＥ，ＥＳ，ＦＩ，ＧＢ，ＧＤ，ＧＥ，ＧＨ，ＧＭ，ＨＲ，ＨＵ，ＩＤ，ＩＬ，ＩＮ，ＩＳ，ＪＰ，ＫＥ，ＫＧ，ＫＰ，ＫＲ，ＫＺ，ＬＣ，ＬＫ，ＬＲ，ＬＳ，ＬＴ，ＬＵ，ＬＶ，ＭＤ，ＭＧ，ＭＫ，ＭＮ，ＭＷ，ＭＸ，ＮＯ，ＮＺ，ＰＬ，ＰＴ，ＲＯ，ＲＵ，ＳＤ，ＳＥ，ＳＧ，ＳＩ，ＳＫ，ＳＬ，ＴＪ，ＴＭ，ＴＲ，ＴＴ，ＵＡ，ＵＧ，ＵＺ，ＶＮ，ＹＵ，ＺＡ，ＺＷ

(72)発明者　エクストロム、ジョセフ・ジェイ
アメリカ合衆国ユタ州84042・リンドン・イースト　300サウス　131
(72)発明者　モス、スティーブン・エス
アメリカ合衆国ユタ州84042・リンドン・ノース　450イースト　298

【要約の続き】
によって制限される。